1. Upgrade Advisor Plan

This upgrade plan is based on AutoSupport received on Sat Jan 02 15:44:49 PST 2021

Serial Number	Cluster Name	Hostname	Partner Hostname	Model No	ONTAP Version
211810000073	**BISPSTON1070**	**BISPSTON1070-C2**	**BISPSTON1070-C1**	**FAS8200**	**9.3P17 Cluster-Mode**

Upgrade Plan Addendum

Please review the *Upgrade Plan Addendum* for additional checks, cautions, frequently asked questions, and errata. Incorporate the addendum information into your upgrade preparation and execution process as appropriate. This is an all-inclusive addendum covering all releases and is not context sensitive.

Download and Install OneCollect today to simplify interoperability checks in the future. If a recent OneCollect file was detected, view a summary of Interoperability items that require remediation at the end of this upgrade plan.

1.1. Information and Warnings

Related to	Information and Warnings Description
Upgrade	**Security Vulnerability Awareness** Please review NetApp's Security Vulnerability Handling and Response Policy as well as any Identified Vulnerabilities that may be applicable to your selected target upgrade revision. This information can be found at https://security.netapp.com/advisory.
Upgrade	**Protocol Considerations** In general, services based on stateless protocols - such as NFSv3, FCP, and iSCSI - are less susceptible to service interruptions during upgrades than session-oriented protocols - such as CIFS and NDMP. This system has the following protocol licenses - **[iSCSI, FCP, NFS, CIFS]**
Upgrade	**Compatibility Review** Confirm interoperability of DSM, NAS Clients (NFS/SMB), SAN Switch OS/ SAN Clients (iSCSI, FCP, FCOE), Backup/Recovery Applications, SnapProtect Server, SnapProtect iDataAgent, and Management Software such as SnapManager or OnCommand Products. You can find the appropriate software/ ONTAP revision supported configuration in the Interoperability Matrix.
Upgrade	**Upgrade considerations for root-data partitioning** Starting with ONTAP 9.0, root-data partitioning and root-data-data-partitioning is supported for some platform models and configurations. This partitioning capability is enabled during system initialization; it cannot be applied to existing aggregates.For information about migrating your data to a node that is configured for root-data partitioning or root-data-data partitioning, contact your account team or partner organization. **Related Information** ONTAP 9.0 Disks and Aggregates Power Guide

Upgrade	**Review Risks across the Cluster** Please check the risk details for your cluster here that might impact your upgrade. **WARNING** These risks may include detected failed disks in the cluster and these conditions may negatively impact the upgrade process. These conditions need to be mitigated before you proceed with an upgrade.
Upgrade	**Guidelines for estimating the duration of the upgrade process** For each HA pair, you should plan for approximately 30 minutes to complete preparatory steps, 60 minutes to perform the upgrade, and 30 minutes to complete post-upgrade steps.
Upgrade	**Load Sharing Mirrors of data volumes stop working on upgrade to ONTAP 9.5 or newer release.** **WARNING** Beginning with ONTAP 9.1, support for the creation of new load-sharing mirrors for data volumes was eliminated. While support for pre-existing load-sharing mirrors for data volumes continued through ONTAP 9.4, this support was completely withdrawn starting with the ONTAP 9.5 release. Creation of load-sharing mirrors for root volume protection continues to be supported as a NetApp best practice. It is recommended that customers decommission load-sharing mirrors for data volumes or contact their account teams and/or technical support for assistance before upgrading to ONTAP 9.5. Possible alternatives to load-sharing mirrors for data volumes include individual SnapMirror relationships, or implementation of FlexCache.
Upgrade	**Hardware Universe Review** Please review the Hardware Universe for platform related considerations for the target ONTAP version. For major releases these considerations likely include an increased root volume size to accommodate successful core and log generation.
Upgrade	**Rate limiting of UDP and IP-fragments affecting NFS clients after upgrades.** Storage administrators can validate the connectivity of a Storage Virtual Machine (SVM, formerly known as Vserver) to configured DNS servers using the `vserver services name-service dns check` command If the node where this command is performed receives sufficient UDP traffic,the response may be dropped by ONTAP even though packet traces confirm that the response was correctly delivered to the storage system.
Upgrade	**Verifying cluster upgrade limits** 1.Verify that the cluster does not exceed the system limits for your platform. NetApp Hardware Universe 2.If your cluster is configured for SAN, verify that it does not exceed the configuration limits for FC, FCoE, and iSCSI. SAN configuration 3.Determine the CPU and disk utilization: `node run -node node_name -command sysstat -c 10 -x 3`

	You should monitor CPU and disk utilization for 30 seconds. The values in the `CPU` and `Disk Util` columns should not exceed 50% for all 10 measurements reported. No additional load should be added to the cluster until the upgrade is complete.
Upgrade	**Systems running BIOS less than 11.5 are vulnerable to BURT 1195243** **WARNING** On some systems, BIOS maps out memory DIMMs that have a correctable ECC (CECC) memory error when the system is initializing. As a result, the system does not boot because some of its system memory is missing. https://mysupport.netapp.com/site/bugs-online/product/ONTAP/BURT/1195243
Upgrade	**NDMP modes for backup and restore operations** You can choose to perform tape backup and restore operations either at a node level (node-scoped NDMP mode) as you have been doing until now or at a Storage Virtual Machine (SVM) level. In the SVM-scoped NDMP mode of operation, NDMP service must be enabled on the SVM. For more information about node-scoped NDMP mode and SVM-scoped NDMP mode, see the Clustered ONTAP Data Protection Tape Backup and Recovery Guide. Please refer the Release Notes for more details.
Upgrade	**Considerations for session-oriented protocols** If you are using session-oriented protocols, consider the following: • CIFS If you configured a Hyper-V over SMB solution, Hyper-V and the contained virtual machines remain online and provide continuous availability during the ONTAP upgrade.For all other CIFS configurations, client sessions are terminated. • NFSv4.x NFSv4.x clients will automatically recover from connection losses experienced during the upgrade using normal NFSv4.x recovery procedures. Applications might experience a temporary I/O delay during this process. You should direct users to end their sessions before you upgrade. • Backups and restores State is lost and the client user must retry the operation. **Attention:**Do not initiate a backup or restore during or immediately before an upgrade. Doing so might result in data loss. • Applications (for example, Oracle or Exchange) Effects depend on the applications. For timeout-based applications, you might be able to change the timeout setting to longer than the ONTAP reboot time to minimize adverse effects.
Upgrade	**Disk Firmware Update** Disk firmware is bundled with the ONTAP system files and updated automatically during ONTAP upgrades. By default, disk firmware updates take place automatically in the background, thus ensuring the continuity of storage system services. **Related information** ONTAP 9.0 Disks and Aggregates Power Guide
Revert	**Security Vulnerability Awareness**

	Please review NetApp's Security Vulnerability Handling and Response Policy as well as any Identified Vulnerabilities that may be applicable to your selected target upgrade revision. This information can be found at https://security.netapp.com/advisory.
Revert	**Authentication for Cluster Peering** All cluster peering relationships are automatically converted to be unauthenticated. If those relationships are to function after the revert action, they must be converted to unauthenticated state on the peered clusters as well(mixed version peers). Once both clusters are reverted, they continue to work as both the clusters' relationships are set as unauthenticated.
Revert	**Reverting clusters to an earlier ONTAP release family** Reversion affects all nodes in the cluster - The reversion must be performed on all nodes in the cluster; however, some of the procedures must be performed on each HA pair and completed on each set of nodes before other pairs are reverted.
Revert	**SnapMirror** Following prerequisites to be performed when reverting from ONTAP 9.7P8 to ONTAP 9.3P17 • Must quiesce all relationships. Allow operations to complete or abort ongoing operations. Break all relationships Revert. • For FleXible Data Protection(Vault) relationship , if common Snapshot copy still exists after revert complete, resync all relationships and resume all relationships. • For Data Protection relationships, • Case 1. The destination volumes were hosted on the node reverted from ONTAP 9.7P8 to ONTAP 9.3P17, while the source volumes still stay on ONTAP 9.7P8 nodes. In this case, the relationship can't be re-established. • Case 2. The source volumes were hosted on the node reverted from ONTAP 9.7P8 to ONTAP 9.3P17, while the destination volumes still stay on ONTAP 9.7P8 nodes. In this case, the relationship can be re-established if common snapshots still exist. • Load-sharing relationship have to be deleted, all destination volumes have to be deleted. • Must disable all network compression attributes in SnapMirror policies • Must delete relationships with FlexClone destination volumes • Must wait for all currently running single file and Snapshot restore operations to complete successfully or abort the restore operations. • All incomplete (request that have failed or have been abort) single file and Snapshot restore requests must be removed by running `SnapMirror restore` with the `clean-up-failure` option. • All ONTAP 9.7P8 SnapMirror policies will be cleaned up under the following procedure: • Delete all Vault relationship that have SnapMirror policy of type `async-mirror` . • Remove `all_source_snapshot` rule from all user created `async-mirror` type policies.

	- If any Vault relationship is using system generated MirrorAndVault policy which is present only in ONTAP 9.7P8, assign different policy of type `mirror-vault` to that relationship. - Disable network compression on all the SnapMirror policies
Revert	**Undelete Volumes** This feature is enabled by default, any deleted volume will appear as pending delete volumes. The pending delete volumes needs to be removed before proceeding to revert. Since the command to purge these volumes is only available in diag mode, the revert-to command would ask to contact NetApp support to perform this operation. The diag level command to be used is volume recovery-queue purge-all.
Revert	**Disk Firmware Update** Disk firmware is bundled with the ONTAP system files and updated automatically during ONTAP upgrades. By default, disk firmware updates take place automatically in the background, thus ensuring the continuity of storage system services. **Related information** ONTAP 9.0 Disks and Aggregates Power Guide

1.2. Upgrade Plan

From ONTAP	To ONTAP
9.3P17 Cluster-Mode	9.7P8 Cluster-Mode

Steps	Upgrade Plan
1	**Review ONTAP 9.7P8 Release Notes and ONTAP 9.7P8 Upgrade Guide** Review ONTAP 9.7P8 Release Notes and the ONTAP 9.7P8 Upgrade Guide for important information and technical detail before beginning your upgrade
2	**Suspending SnapMirror operations** **WARNING** Cluster BISPSTON1070 is running SnapMirror. To prevent SnapMirror transfers from failing, you must suspend SnapMirror operations and upgrade destination nodes before upgrading source nodes. (i) Suspend SnapMirror transfers for a destination volume (ii) Upgrade the node that contains the destination volume (iii) Upgrade the node that contains the source volume (iv) Resume the SnapMirror transfers for the destination volume. **Note:** SnapMirror transfers for all other destination volumes can continue while the nodes that contain the original destination and source volumes are upgraded.

3	**Ensuring that no jobs are running**
	You must verify the status of cluster jobs before upgrading or downgrading to a different ONTAP release. If any aggregate, volume, NDMP (dump or restore), or Snapshot jobs (such as create, delete, move, modify, replicate, and mount jobs) are running or queued, allow the jobs to finish successfully or stop the queued entries.
	(a) Review the list of any running or queued aggregate, volume, or Snapshot jobs:
	`job show`
	WARNING:
	Do not delete dedupe job which is running / queued as it will affect future sis policy jobs.
	Refer Customer Public Report on NetApp Support Site for more details.
	(b) Delete any running or queued aggregate, volume, or Snapshot copy jobs:
	`job delete -id job_id`
	(c) Ensure that no aggregate, volume, or Snapshot jobs are running or queued:
	`job show`

4	**Obtaining ONTAP software images** **Before you begin:** You must copy a software image from the NetApp Support Site to an HTTP or FTP server on your network so that nodes can access the image. For upgrades from ONTAP 9.3 to ONTAP 9.7, you must download both ONTAP 9.5 and ONTAP 9.7 images.

1. The target ONTAP software can be downloaded from **Software Downloads** area of the NetApp Support Site
2. Copy the software image (for example, 900_q_image.tgz) from the NetApp Support Site to the directory on the HTTP or FTP server from which the image will be served.

Related information

NetApp Downloads: Software

Note : For systems with NVE, you must download the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption. If you use the ONTAP software image for restricted countries to upgrade a system with NetApp Volume Encryption, the system panics and you lose access to your volumes

5

Upgrading ONTAP cluster nondisruptively by using the automated method

Before you begin:

Note: Do not perform operations like cluster unjoin and node rename when the automated upgrade is in progress. If you are planning to perform cluster unjoin and node rename operations, before initiating an upgrade, remove all ONTAP images from the package repository:

```
cluster image package delete
```

- You must have satisfied upgrade preparation requirements.
- For each HA pair, each node should have one or more ports on the same broadcast domain. When a set of nodes is upgraded during a batch upgrade, the LIFs are migrated to the HA partner nodes. If the partners do not have any ports in the same broadcast domain, then the LIF migration fails.

If you do not plan to monitor the progress of the upgrade process:

1.Trigger an AutoSupport notification:

```
autosupport invoke -node * -type all -message
"MAINT=<time>h Starting_NDU"
```

where <time> is the maintenance window duration for the upgrade.

NOTE: During this time, automatic case creation will suppressed at NetApp. You can resume case creation at any time by executing the following command:

```
system node autosupport invoke -node * -type all -message
"MAINT=END"
```

To learn more about suppressing case creation during maintenance windows, refer to this KB Article on the NetApp Support site.

2.Download the target ONTAP software package:

```
cluster image package get -url location
```

Note: If you are upgrading from ONTAP 9.3 to 9.7, download the software package for both ONTAP 9.5, and then use the same command to download the software package for 9.7.

3.Verify that the software package is available in the cluster package repository:

```
cluster image package show-repository
```

4.Verify that the cluster is ready to be upgraded nondisruptively:

```
cluster image validate -version package_version_number
```

5.Optional: If desired, generate a software upgrade estimate:

```
cluster image update -version package_version_number -estimate-only
```

6.Perform the software upgrade:

```
cluster image update -version package_version_number
```

This command validates that each cluster component is ready to be upgraded, installs the target ONTAP image on each node in the cluster, and then performs a nondisruptive upgrade in the background. If an issue is encountered, the update pauses and prompts you to take corrective action.

Note: If you are upgrading from ONTAP 9.3 to 9.7, use the 9.7 package_version_number in the above command. The automated upgrade process uses the 9.5 image in the background to complete the update to 9.7. It is not necessary for you to upgrade to 9.5, then do a separate upgrade to 9.7.

You can use the `cluster image show-update-progress` command to view details about the issue. After correcting the issue, you can resume the update by using the `cluster image resume-update` command.

If the cluster consists of 2 through 6 nodes, a rolling upgrade is performed.

If the cluster consists of 8 or more nodes, a batch upgrade is performed by default. If desired, you can use the `-force-rolling` parameter to specify a rolling upgrade instead.

After completing each takeover and each giveback, the upgrade waits for 8 minutes to enable client applications to recover from the pause in I/O that occurs during the takeover and giveback.

If your environment requires more or less time for client stabilization, you can use the `-stabilize-minutes` parameter to specify a different amount of stabilization time.

7.Optional: If necessary, manage the upgrade process:

a.To Monitor the status and estimated duration of the upgrade, enter this command

```
cluster image show-update-progress
```

b.To view the log of each task that has executed during the upgrade, enter this command

```
cluster image show-update-log
```

c.To pause the upgrade, enter this command

```
cluster image pause-update
```

d.To resume a paused upgrade, enter this command

```
cluster image resume-update
```

e.To cancel the upgrade, enter this command

```
cluster image cancel-update
```

8.Display the cluster update history to verify that the upgrade was completed successfully for each node:

```
cluster image show-update-history
```

9.Trigger an AutoSupport notification:

```
autosupport invoke -node * -type all -message "MAINT=END Finishing_NDU"
```

If your cluster is not configured to send AutoSupport messages, a copy of the notification is saved locally.

1.3. Backout Plan

From ONTAP	To ONTAP
9.7P8 Cluster-Mode	9.6P9

Note: Please note that direct revert from ONTAP 9.7P8 to ONTAP 9.3P17 is not allowed. You must perform a revert from 9.7P8 to 9.6P9

Steps	Backout Plan Description

1	**Verifying Storage health**
	Determine if any disk drives are broken, undergoing maintenance, or reconstructing:
	a. Display any broken disks:
	`storage disk show -state broken`
	b. Remove or replace any broken disks.
	c. Display any disks in maintenance, pending, or reconstructing states:
	`storage disk show -state maintenance|pending|reconstructing`
	d. Wait for the maintenance or reconstruction operation to complete before proceeding.

2	**Preparing Snapshot copies before reverting** **NOTE:** Before reverting to an earlier ONTAP release, you must disable all Snapshot copy policies and delete any Snapshot copies that were created after upgrading to the current release. **Before you begin** If you are reverting in a SnapMirror environment, you must first have deleted the following mirror relationships: • All load-sharing mirror relationships • Any data protection mirror relationships that were created in ONTAP 9.7P8 • All data protection mirror relationships if the cluster was re-created in ONTAP 9.7P8 **(1)** Disable Snapshot copy policies for all data SVMs: `volume snapshot policy modify -vserver * -enabled false` **(2)** Disable Snapshot copy policies for each node's root aggregate: a. Identify the node's root aggregate by using the `run -node nodename aggr status` command. b. Disable the Snapshot copy policy on the root aggregate `run -node nodename aggr options root_aggr_name nosnap on` c.Repeat this step for each remaining node. **(3)** Disable Snapshot copy policies for each node's root volume: a. Identify the node's root volume by using the `run -node nodename vol status` command.You identify the root volume by the word root in the Options column of the vol status command output. b.Disable the Snapshot copy policy on the root volume:

	`run -node` *`nodename`* `vol options` *`root_volume_name`* `nosnap on`
	c.Repeat this step for each remaining node.
	(4) Set the privilege level to advanced:
	`set -privilege advanced`
	(5) Delete all Snapshot copies that were created after upgrading to the current release:
	`volume snapshot prepare-for-revert -node` *`nodename`*
	This command deletes the newer-version Snapshot copies on each data volume, root aggregate, and root volume.
	(6) Repeat Step 5 for each remaining node.
	(7) Return to the admin privilege level:
	`set -privilege admin`

3	**Reversion process considerations** **WARNING** **(a)** Reversion is disruptive **(b)** Reversion affects all nodes in the cluster **(c)** The reversion is complete when all nodes are running the new target release **(d)** If you are unable to complete the reversion for any reason, contact technical support immediately. If you have reverted some, but not all, of the nodes, do not attempt to upgrade the cluster back to the source release. **(e)** When you revert a node, it clears the cached data in a Flash Cache module **(f)** After you enter the system node revert-to command to revert a cluster, the version command becomes unavailable and does not display any output until the reversion is completed.
4	**Considerations for whether to manually update the SP firmware** **WARNING** The SP automatic update functionality is disabled, you must manually update the SP firmware to a version that is supported for the ONTAP version you reverted or downgraded to.

5	**Reverting ONTAP cluster**
	(a) Verify that the target ONTAP software is installed:
	`system node image show`
	(b) Set the node's target ONTAP software image to be the default image:
	`system image modify -node` *`nodename`* `-image` *`target_image`* `-isdefault true`
	(c) Verify that the target ONTAP software image is set as the default image:
	`system node image show`
	(d) Set the privilege level to advanced:
	`set -privilege advanced`
	(e) If the cluster consists of only two nodes, verify that the node does not hold epsilon:
	1.Check whether the node currently holds epsilon:
	`cluster show -node` *`nodename`*
	2.If the node holds epsilon, mark epsilon `false` on the node so that epsilon can be transferred to the node's partner:
	`cluster modify -node` *`BISPSTON1070-C2`* `-epsilon false`

3.Transfer epsilon to the node's partner by marking epsilon true on the partner node:

```
cluster modify -node BISPSTON1070-C1 -epsilon true
```

(f) Disable storage failover for the nodes in the HA pair from either node

```
storage failover modify -node nodename -enabled false
```

You only need to disable storage failover once for the HA pair. When you disable storage failover for a node, storage failover is also disabled on the node's partner.

Log in to the node that you want to revert.

To revert a node, you must be logged in to the cluster through the node's node management LIF

(g) Set the privilege level to advanced

```
set -privilege advanced
```

(h) Verify that the node is ready for reversion

```
system node revert-to -node nodename -check-only true -version 9.3
```

- The check-only parameter identifies any preconditions that must be addressed before reverting, such as the following examples:
  - Disabling storage failover
  - Disabling the Snapshot policy
  - Deleting Snapshot copies that were created after upgrading to the later release family
- Proceed to the next step when all identified preconditions have been addressed

(i) Verify that all of the preconditions have been addressed

```
system node revert-to -node nodename -check-only true -version 9.3
```

(j) Revert the cluster configuration of the node

```
system node revert-to -node nodename -version 9.3
```

The -version option refers to the target release family. For example, if the software you installed and verified in Step (b) is Data ONTAP 8.3.1, the correct value of the -version option is 8.3

The cluster configuration is reverted, and then you are logged out of the clustershell.

(k) Log back into the clustershell, and then switch to the nodeshell

```
system node run -node nodename
```

(l) Revert the filesystem configuration of the node

```
revert_to 9.3
```

This command verifies that the node's filesystem configuration is ready to be reverted and then reverts it.

If any preconditions are identified, you must address them and then reenter the revert_to command

When the command finishes, the LOADER prompt is displayed.

(m) At the LOADER prompt, enter the following command to boot to the target release

```
boot_ontap
```

(n) Repeat Steps (h) through (m) on the other node in the HA pair.

(o) If the cluster consists of only two nodes, reenable cluster HA

```
cluster ha modify -configured true
```

(p) Reenable storage failover on both nodes if it was previously disabled

```
storage failover modify -node nodename -enabled true
```

	(q) Verify that the cluster is in quorum and that services are running by using the `cluster show` and `cluster ring show` (advanced privilege level) commands. You should do this before reverting any additional HA pairs. **(r)** Repeat Steps (f) through (q) for each additional HA pair in the cluster. **(s)**After all nodes have been reverted, reinstall the ONTAP 9.3 image as the alternate image on each node: `system image update -node * -package location -background true` You do not need to boot the image. Reinstalling the ONTAP 9.3 image puts the cluster in a state that is necessary for the SVM networking to be verified when you are ready to upgrade back to ONTAP 9.7P8.

6	**Preparing Snapshot copies after reverting**
	After reverting to an earlier version of ONTAP, you must enable Snapshot copy policies to start creating Snapshot copies again.
	1. Enable Snapshot copy policies for all data SVMs:
	`volume snapshot policy modify -vserver * -enabled true`
	2. For each node, enable the Snapshot copy policy of the root volume:
	`run -node nodename vol options root_vol_name nosnap off`
	3. For each node, enable the Snapshot copy policy of the aggregates:
	`run -node nodename aggr options aggr_name nosnap off`

7	**Considerations for dump backups** If you use the dump engine to back up FlexVol volumes, then after reverting to ONTAP 9.3P17, you must perform a baseline backup operation before you can perform any incremental backup operations. **Related information** Clustered ONTAP 9.0 Data Protection Tape Backup and Recovery Guide

8	**Verifying IPv6 firewall entries**
	A reversion from ONTAP 9.7P8 might result in missing default IPv6 firewall entries for some services in firewall policies. You need to verify that the required firewall entries have been restored to your system.
	1. Verify that all firewall policies are correct by comparing them to the default policies:
	`system services firewall policy show`
	2. Manually add any missing default IPv6 firewall entries by creating a new firewall policy:
	`system services firewall policy create`
	3. Apply the new policy to the LIF to allow access to a network service:
	`network interface modify`